PN - JP2000041039 A 20000208

PD - 2000-02-08

PR - JP19980209238 19980724

OPD - 1998-07-24

TI - DEVICE AND METHOD FOR MONITORING NETWORK

IN - KURATA MASAHIKO;MACHIDA NAOYOSHI;TAKESADA MUTSUHARU;YAMAGISHI NORIKAZU

PA - HITACHI ELECTRONICS SERVICE CO

IC - H04L12/24 ; H04L12/26 ; H04L12/56

TI - Network abnormality monitoring apparatus records operation condition of network detected at regular intervals and compares recorded data with current operation condition to detect abnormality

PR - JP19980209238 19980724

PN - JP2000041039 A 20000208 DW200018 H04L12/24 011pp

PA - (NIDE-N) NIPPON DENSHI SERVICE KK

IC - H04L12/24 ;H04L12/26 ;H04L12/56

AB - JP2000041039 NOVELTY - A measurement unit (100) measures the network operating condition in addition to analyzing packet data. The network condition recorded at regular intervals is set as standard data. The network condition measured currently is compared with said standard data based on which a decision unit (230) judges an abnormality. DETAILED DESCRIPTION - An INDEPENDENT CLAIM is also included for network abnormality monitoring procedure.

- USE - For monitoring abnormality in network.
- ADVANTAGE - As network conditions in previous time periods is used for judging abnormality, the experience of network management etc. is no more required. DESCRIPTION OF DRAWING(S) - The figure shows the block diagram of network abnormality monitoring apparatus. (100) Measurement unit; (230) Decision unit.
- (Dwg.1/4)

OPD - 1998-07-24

AN - 2000-202796 [18]

PN - JP2000041039 A 20000208

PD - 2000-02-08

AP - JP19980209238 19980724

IN - MACHIDA NAOYOSHI;KURATA MASAHIKO;YAMAGISHI NORIKAZU;TAKESADA MUTSUHARU

PA - HITACHI ELECTRONICS SERVICE CO LTD

TI - DEVICE AND METHOD FOR MONITORING NETWORK

AB - PROBLEM TO BE SOLVED: To provide a network monitoring device capable of setting the reference of abnormality judgement from the operation result in the past.

- SOLUTION: The operating state of a network1 is measured from packet data on the network 1 by an operating state measuring part 100, the measured operating state is estimated by an estimation part 210, the threshold value of abnormality judgement concerning the network 1 is set based on the estimated operating state by a threshold value setting part 220, a discrimination part 230 compares the operating state measured by the operating state measuring part 100 with the threshold value set by the threshold value setting part 220 and measures whether the operating state is abnormal or not and when the discrimination part230 discriminates abnormality, it is reported by a reporting part320.

I - H04L12/24 ;H04L12/26 ;H04L12/56

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2000－41039
（P2000－41039A）
(43)公開日　平成12年２月８日(2000.2.8)

(51)Int.Cl.⁷	識別記号	ＦＩ		テーマコード（参考）
Ｈ０４Ｌ　12/24		Ｈ０４Ｌ　11/08		５Ｋ０３０
12/26		11/20	１０２Ｚ	
12/56				

審査請求　未請求　請求項の数10　ＯＬ　（全 11 頁）

(21)出願番号　特願平10－209238

(22)出願日　平成10年７月24日(1998.7.24)

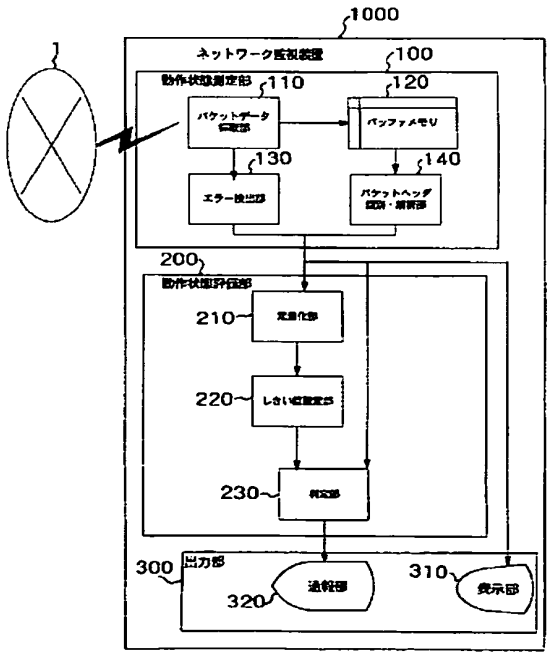
(71)出願人　000233491
日立電子サービス株式会社
神奈川県横浜市戸塚区品濃町504番地２
(72)発明者　町田　直義
神奈川県横浜市戸塚区品濃町504番地２
日立電子サービス株式会社内
(72)発明者　倉田　真彦
神奈川県横浜市戸塚区品濃町504番地２
日立電子サービス株式会社内
(74)代理人　100087170
弁理士　富田　和子　（外１名）

最終頁に続く

(54)【発明の名称】　ネットワーク監視装置および方法

(57)【要約】
【課題】　異常判断の基準を過去の動作実績から設定することができるネットワーク監視装置を提供する。
【解決手段】　ネットワーク１上のパケットデータから動作状態測定部１００によってネットワーク１の動作状態を測定し、既に測定された動作状態を定量化部２１０によって定量化し、定量化された動作状態に基づいてネットワーク１についての異常判断のしきい値をしきい値設定部２２０により設定し、上記動作状態測定部１００で測定される動作状態を上記しきい値設定部２２０により設定されたしきい値とを判定部２３０で比較して動作状態が異常か否かを測定し、判定部２３０で異常と判定されたとき、その旨を通報部３２０によって通報する。

図1



【特許請求の範囲】
【請求項１】監視対象とするネットワークに送出されたパケットデータを採取するための採取手段と、
上記パケットデータを解析してネットワークの動作状態を測定するための測定手段と、
期間を指示する操作を受付け、当該指示された期間に測定された複数時点における動作状態を標準として、異常判定の基準を設定するための設定手段と、
上記測定される動作状態を上記設定された基準と対比して、ネットワークが異常か否かを判定するための判定手段と、
上記ネットワークが異常であると判定されたとき、これを通報するための通報手段とを備えることを特徴とするネットワーク監視装置。
【請求項２】監視対象とするネットワークに送出されたパケットデータを採取するための採取手段と、
上記パケットデータを解析してネットワークの動作状態を測定するための測定手段と、上記既に測定された複数時点における動作状態についての代表値および散布度を求め、これらに基づいて異常判定の基準を設定するための設定手段と、
上記代表値および上記測定される動作状態の差が、上記散布度に対して有意であるとき、ネットワークが異常であると判定するための判定手段と、
上記ネットワークが異常であると判定されたとき、これを通報するための通報手段とを備え、
を特徴とするネットワーク監視装置。
【請求項３】　請求項２に記載のネットワーク監視装置において、
上記設定手段は、上記既に測定された複数時点における動作状態を、一定の周期に対し、周期相互に積算して代表値および散布度を上記周期における少なくとも１の位相について求め、
上記判定手段は、上記測定される動作状態と、対応する位相の代表値および散布度に基づいて判定することを特徴とするネットワーク監視装置。
【請求項４】　請求項３に記載のネットワーク監視装置において、
上記設定手段は、上記測定される動作状態の時系列変化から周期を設定するための周期設定手段を備えることを特徴とするネットワーク監視装置。
【請求項５】　請求項４に記載のネットワーク監視装置において、
上記周期設定手段は、
上記測定される動作状態の時系列変化における繰り返しを検知し、検知された繰り返しのそれぞれの周期を求めるための繰り返し検出手段と、
上記それぞれ求められた周期を表示し、いずれかを指定する操作を受け付けるためのインタフェース手段と、
上記指定された周期を上記周期として設定するための手段とを備えることを特徴とするネットワーク監視装置。
【請求項６】　請求項２から５のいずれか一項に記載のネットワーク監視装置において、
上記測定手段は、パケットデータが採取されたときのネットワークの性能で規格化した動作状態を求めるための規格化手段を備えることを特徴とするネットワーク監視装置。
【請求項７】監視対象とするネットワークに送出されたパケットデータを採取するための採取手段と、
上記パケットデータを解析してネットワークの動作状態を測定するための測定手段と、
既に測定された複数時点における動作状態を標準として、異常判定の基準を設定するための設定手段と、
上記測定される動作状態を上記設定された基準と対比して、ネットワークが異常か否かを判定するための判定手段と、
上記ネットワークが異常であると判定されたとき、これを通報するための通報手段とを備え、
上記測定手段は、予め指定された端末から送出されたパケットデータについての動作状態を求めるための弁別手段を備えることを特徴とするネットワーク監視装置。
【請求項８】監視対象とするネットワークに送出されたパケットデータを採取するための採取手段と、
上記パケットデータを解析してネットワークの動作状態を測定するための測定手段と、
既に測定された複数時点における動作状態を標準として、異常判定の基準を設定するための設定手段と、
上記測定される動作状態を上記設定された基準と対比して、ネットワークが異常か否かを判定するための判定手段と、
上記ネットワークが異常であると判定されたとき、これを通報するための通報手段とを備え、
上記判定手段は、
各時点に測定される動作状態について異常か否かを判定する第１の判定段階と、
上記第１段階で異常と判定された動作状態が予め定められた頻度を超えて発生するか否かを判定する第２の判定段階とを有する判定を行って動作状態の異常を判定することを特徴とするネットワーク監視装置。
【請求項９】監視対象とするネットワークに送出されたパケットデータを採取し、
上記採取したパケットデータを解析してネットワークの動作状態を測定し、
上記既に測定した複数時点における動作状態についての代表値および散布度を求め、
上記代表値および上記測定する動作状態の差が、上記散布度に対して有意であるとき、ネットワークが異常であると判定し、
上記ネットワークが異常であると判定したとき、これを通報することを特徴とするネットワーク監視方法。

【請求項１０】　情報処理装置を用いてネットワークの動作状態を監視するためのプログラムが格納された記憶媒体において、
上記プログラムは、
監視対象とするネットワークに送出されたパケットデータを採取するための処理と、
上記パケットデータを解析してネットワークの動作状態を測定するための処理と、
既に測定された複数時点における動作状態から、当該ネットワークにおける異常判定の基準を設定するための処理と、
上記測定される動作状態を上記設定された基準と対比して、ネットワークが異常か否かを判定するための処理と、
上記ネットワークが異常であると判定されたとき、これを通報するための処理とを上記情報処理装置を用いて実行するためのものであることを特徴とするプログラムが格納された記憶媒体。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は、ネットワークの異常を検出するためのネットワーク監視装置および方法に係り、特に、対象のネットワークに応じた基準で異常を検出することができるネットワーク監視装置および方法に関する。
【０００２】
【従来の技術】従来、ＳＮＭＰ（Simple Network Management Protocol、簡易ネットワーク管理プロトコル）を用いた管理マネージャがネットワークを監視するために用いられている。
【０００３】ＳＮＭＰは、管理ステーション上の「マネージャ」からの処理要求に対して、管理対象システム上の「エージェント」がＭＩＢ（Management Information Base、管理情報データベース）に蓄積されている、ＳＮＭＰ情報をマネージャに通知するという、マネージャ／エージェント・モデルである。このため上述のマネージャでは、ＳＮＭＰ情報をＭＩＢから読み出すことに伴い新たなトラフィックを発生させ、ネットワークの負荷を増大させるという問題がある。
【０００４】一方、ネットワークに送出されたパケットデータをモニタするテスタやアナライザなどが、ネットワーク管理者等によって利用されている。パケットデータのモニタは、ネットワークに新たなトラフィックを発生させずに行えるため、対象とするネットワークに負荷を与えずに監視することができる。
【０００５】このようなアナライザでは、ネットワーク上のパケットを蓄積するためのバッファメモリ、および、蓄積されているパケットの解析を支援する機能を備えている。
【０００６】また、上記テスタの中には、監視の対象とする項目と、項目毎の評価の基準とを作業者が予め設定することによって、基準を超えた項目等を表示することができるものも開発されている。
【０００７】
【発明が解決しようとする課題】上述のアナライザですべてのパケットを蓄積することは、バッファメモリの記憶容量などの制限から現実的ではなく、ネットワーク管理者が、その経験から、蓄積すべきパケットの種別、期間などを指定して運用することが多い。
【０００８】一方、障害の切り分け、動作状態の解析などは、それに必要なパケットがアナライザのバッファメモリに残っていなければならない。ところが、実際の障害発生時には、発生した障害が予期しないものであるなどして、必要なパケットが蓄積されているケースは稀である。従って、蓄積すべきパケットの種別等を指定しなおすなどして、障害の再発を待たなければならないという問題がる。特に、インタミテント障害では、その解析に多大な時間を要するという問題がある。
【０００９】また、上記テスタにおける項目および基準の設定は、利用者によってなされなければならない。この設定には、ネットワークに関する知識や保守・管理における経験が要求され、また、基準を超えた旨が表示された項目からネットワークの状態を判断する能力も要求される。このため、上記テスタを利用してのネットワークの状態の把握は、ネットワーク管理のスペシャリスト等でなければ困難である。
【００１０】本発明は、監視の対象とするネットワークの状態に応じて監視の基準を設定することができる監視装置および方法を提供することを目的とする。
【００１１】
【課題を解決するための手段】上記目的を達成するために、本発明の第１の態様によれば、監視対象とするネットワークに送出されたパケットデータを採取するための採取手段と、上記パケットデータを解析してネットワークの動作状態を測定するための測定手段と、期間を指示する操作を受付け、当該指示された期間に測定された複数時点における動作状態を標準として、異常判定の基準を設定するための設定手段と、上記測定される動作状態を上記設定された基準と対比して、ネットワークが異常か否かを判定するための判定手段と、上記ネットワークが異常であると判定されたとき、これを通報するための通報手段とを備えることを特徴とするネットワーク監視装置が提供される。
【００１２】本発明の第２の態様によれば、監視対象とするネットワークに送出されたパケットデータを採取するための採取手段と、上記パケットデータを解析してネットワークの動作状態を測定するための測定手段と、上記既に測定された複数時点における動作状態についての代表値および散布度を求め、これらに基づいて異常判定の基準を設定するための設定手段と、上記代表値および

上記測定される動作状態の差が、上記散布度に対して有意であるとき、ネットワークが異常であると判定するための判定手段と、上記ネットワークが異常であると判定されたとき、これを通報するための通報手段とを備え、を特徴とするネットワーク監視装置が提供される。

【００１３】ここで、上記設定手段において、上記既に測定された複数時点における動作状態を、一定の周期に対し、周期相互に積算して位相ごとの代表値および散布度を求め、上記判定手段において、上記測定される動作状態と、対応する位相の代表値および散布度に基づいて判定する構成としてもよい。

【００１４】また、上記設定手段に、上記測定される動作状態の時系列変化から周期を設定するための周期設定手段を備える構成としてもよい。

【００１５】また、上記周期設定手段は、上記測定される動作状態の時系列変化における繰り返しを検知し、検知された繰り返しのそれぞれの周期を求めるための繰り返し検出手段と、上記それぞれ求められた周期を表示し、いずれかを指定する操作を受け付けるためのインタフェース手段と、上記指定された周期を上記周期として設定するための手段とを備える構成とすることができる。

【００１６】本発明の第３の態様によれば、監視対象とするネットワークに送出されたパケットデータを採取するための採取手段と、上記パケットデータを解析してネットワークの動作状態を測定するための測定手段と、既に測定された複数時点における動作状態を標準として、異常判定の基準を設定するための設定手段と、上記測定される動作状態を上記設定された基準と対比して、ネットワークが異常か否かを判定するための判定手段と、上記ネットワークが異常であると判定されたとき、これを通報するための通報手段とを備え、上記測定手段は、予め指定された端末から送出されたパケットデータについての動作状態を求めるための弁別手段を備えることを特徴とするネットワーク監視装置が提供される。

【００１７】本発明の第４の態様によれば、監視対象とするネットワークに送出されたパケットデータを採取するための採取手段と、上記パケットデータを解析してネットワークの動作状態を測定するための測定手段と、既に測定された複数時点における動作状態を標準として、異常判定の基準を設定するための設定手段と、上記測定される動作状態を上記設定された基準と対比して、ネットワークが異常か否かを判定するための判定手段と、上記ネットワークが異常であると判定されたとき、これを通報するための通報手段とを備え、上記判定手段は、各時点に測定される動作状態について異常か否かを判定する第１の判定段階と、上記第１段階で異常と判定された動作状態が予め定められた頻度を超えて発生するか否かを判定する第２の判定段階とを有する判定を行って動作状態の異常を判定することを特徴とするネットワーク監視装置が提供される。

【００１８】本発明の第５の態様によれば、監視対象とするネットワークに送出されたパケットデータを採取し、上記採取したパケットデータを解析してネットワークの動作状態を測定し、上記既に測定した複数時点における動作状態についての代表値および散布度を求め、上記代表値および上記測定する動作状態の差が、上記散布度に対して有意であるとき、ネットワークが異常であると判定し、上記ネットワークが異常であると判定したとき、これを通報することを特徴とするネットワーク監視方法が提供される。

【００１９】本発明の第６の態様によれば、情報処理装置を用いてネットワークの動作状態を監視するためのプログラムが格納された記憶媒体において、上記プログラムは、監視対象とするネットワークに送出されたパケットデータを採取するための処理と、上記パケットデータを解析してネットワークの動作状態を測定するための処理と、既に測定された複数時点における動作状態から、当該ネットワークにおける異常判定の基準を設定するための処理と、上記測定される動作状態を上記設定された基準と対比して、ネットワークが異常か否かを判定するための処理と、上記ネットワークが異常であると判定されたとき、これを通報するための処理とを上記情報処理装置を用いて実行するためのものであることを特徴とするプログラムが格納された記憶媒体が提供される。

【００２０】

【発明の実施の形態】以下、図面を参照して、本発明の実施の形態について説明する。

【００２１】まず、図１を参照して、本発明を適用したネットワーク監視装置の構成について説明する。

【００２２】図１において、ネットワーク監視装置１００は、監視対象とするネットワーク１の動作状態を測定するための動作状態測定部１００と、測定された動作状態を評価するための動作状態評価部２００と、測定または評価された結果を出力するための出力部３００とを有して構成される。

【００２３】上記動作状態測定部１００は、ネットワーク１に送出されたパケットデータを採取するためのパケットデータ採取部１１０と、採取したパケットデータを一旦蓄積するためのバッファメモリ１２０と、上記パケットデータ採取部１１０で採取されたパケットデータのエラーを検出するためのエラー検出部１３０と、上記バッファメモリ１２０に蓄積されているパケットデータを解析するためのパケットヘッダ識別・解析部１４０とを有して構成される。

【００２４】上記パケットデータ採取部１１０は、ネットワーク１の伝送媒体と接続するためのコネクタと、伝送媒体における物理インタフェースと、伝送媒体を伝送される信号からパケットデータ採取するためのフレームキャプチャとを有して構成することができる。より具体

的には、フレームキャプチャは、伝送媒体を伝送される信号、信号をコネクタを介して検出するためのパルス受信機能と、パケットデータについて定められるデータ構造に基づいて、個々のパケットデータを抽出するパケット抽出機能とを備える。

【００２５】上記バッファメモリ１２０は、上記パケットデータ採取部１１０からのダイレクトメモリアクセス（ＤＭＡ）によってパケットデータを受け付ける。そして、各パケットデータごとにタイムスタンプを付して格納する。

【００２６】上記エラー検出部１３０は、上記パケットデータ採取部１１０から受け付ける各パケットデータについて、エラーの検出を行う。例えば、パケットデータ相互の衝突（コリジョン）の検出、パケットデータ長の過不足の検出（ショートパケット、ロングパケットの検出）、データのビット数の過不足（Alignment)不良、および、巡回冗長検査（CRC）による符号誤りの検出等を行う。衝突の検出においては、多重衝突、ジャム（ＪＡＭ）信号、および、遅延衝突（レイトコリジョン）等の検出も行う。

【００２７】上記パケットヘッダ・識別解析部１４０は、上記バッファメモリ１２０から格納されているパケットデータを読み出し、プロトコルの認識、送出クライアントの識別、および、通信ペアの識別を行うとともに、付されているタイムスタンプを読みとる。

【００２８】上記プロトコルの認識においては、プロトコルの種別、フレームサイズ、フレーム数を認識する。

【００２９】また、上記識別した送出クライアントおよびタイムスタンプから、クライアントごとのアクセス間隔を測定する。

【００３０】そして、上記識別した通信ペアから、状態遷移のフロー追跡、再送回数の計測を行い、さらに、上記タイムスタンプを併せて用いて、応答時間を測定する。

【００３１】また、上記送出クライアントの情報を用いて、特定の送出クライアントまたは特定の属性を有する送出クライアントについて弁別するためのフィルタ機能を設けることができる。

【００３２】例えば、特定の送出クライアントに関して弁別することにより、新規に接続されたクライアント、過去にネットワーク障害を引き起こしたことがあるクライアント等に着目して情報を収集することができる。

【００３３】また、クライアントの属性に関して弁別することにより、ネットワーク上の特定の構成要素に属するクライアントや、他のクライアントにサービスを提供するクライアント（サーバ）などについて着目して情報を収集することが可能となる。例えば、他のクライアントからのアクセス頻度が高いことが想定されるファイルサーバ、メールサーバ、ドメインネームサーバ等のサーバ機能を有するクライアントに着目した情報や、特定のハブ、ルータ等の配下にあるクライアント群についての情報を収集することが可能となる。

【００３４】上記動作状態としては、例えば、性能、応答時間、再送時間、および、エラー発生率などのパラメータについて測定することができる。

【００３５】上記性能は、端末間での通信リンクが確立している間に転送されたデータ量Ｍ（ビット数）と、リンクが確立していた時間Ｔとから、次式に基づいて算出する。

【００３６】性能Ｓ＝Ｍ／Ｔ（ｂｐｓ）

上記応答時間は、端末間でのデータ送受において、データを送出した後にその応答データが戻ってくるまでの時間によって測定する。

【００３７】上記再送回数は、端末間の通信リンクが確立している間に、再送が発生した回数を、通信リンクが確立していた時間で除して求めた単位時間あたりの再送回数として計数する。

【００３８】上記エラー発生率は、単位時間あたりのエラー発生数であって、端末間の通信リンクが確立している間に発生したエラー回数を、通信リンクが確立していた時間で除して求める。

【００３９】また、上記応答時間、再送時間、および、エラー発生率などを、上記性能で規格化してもよい。

【００４０】上記動作状態評価部２００は、上記動作状態測定部１００で測定された動作状態を定量化するための定量化部２１０と、定量化された動作状態に基づいて、異常検出のしきい値を設定するためのしきい値設定部２２０と、上記動作状態測定部１００で測定される動作状態が異常か否かを、上記しきい値設定部２２０で設定されたしきい値に基づいて判定するための判定部２３０とを有して構成される。

【００４１】上記定量化部２１０は、上記測定された動作状態を複数時点において取得し、これを統計処理して定量化する。例えば、複数時点における動作状態を母集団として、その代表値および散布度を求めることができる。より具体的には、上記代表値としては標本平均を、上記散布度としては標本標準偏差を求める。なお、上記代表値として、標本中央値、標本モードおよび標本モード等を用いてもよいし、上記散布度として、標本分散、標本平均偏差、標本四分偏差および標本範囲等を用いてもよい。

【００４２】上記標本平均を求めるに際し、例えば、指定された期間について移動平均をとって求めてもよいし、もしくは、指定された周期ごとに積算平均をとって求めてもよい。なお、これらの平均を求めるに際し、期間内の時刻（周期における位相）に応じた重み付けを行って平均することができる。例えば、最近に測定された動作状態ほど大きな重みを付けて移動平均をとってもよいし、最近の積算周期ほど大きな重みを付けて周期毎の積算平均をとってもよいことが可能となる。

【００４３】また、動作状態を標本として抽出する対象となる測定時点の指定するためには、外部から対象となる時点であることを指示する操作を受け付けてもよいし、定量化部２１０において、予め設定された規則に従って指定してもよい。

【００４４】例えば、外部からの操作を受け付けるためのインタフェースを備え、当該インタフェースによって指示が与えられているときに測定された動作状態を抽出したり、上記インタフェースによって指定された始期から終期までの間に測定された動作状態を抽出することができる。このようにして抽出すべき時点を指定することによって、監視対象とするネットワーク１が正常に動作しているときの動作状態を異常検出の基準を設定するための標本として抽出することができる。例えば、ネットワーク１の新規構成または構成変更に伴う初期不良が解消されたと思われる時点から（誤った設定、設定漏れなどの修正、物理的な接続不良の回復などを行ってから）、測定される動作状態を抽出して、これらに基づいて、異常検出の基準を設定することが可能となる。

【００４５】また、上記定量化部２１０において抽出対象の測定時点を指定するためには、例えば、予め定められた長さを有する最近の期間とすること、測定される動作状態の時間変化の周期性を検出し、その周期によって指定することができる。

【００４６】上記しきい値設定部２２０は、上記定量化部２１０によって定量化された統計量に基づいて異常検出のしきい値を設定する。例えば、代表値として標本平均が、散布度として標本標準偏差が与えられるとき、標本平均から標本標準偏差の２倍の距離にしきい値を設定する。

【００４７】上記判定部２３０は、上記動作状態測定部１００で測定される動作状態と、上記しきい値設定部２２０で設定されたしきい値とを比較し、上記測定される動作状態がしきい値を超えるとき、その動作状態が異常であると判定する。

【００４８】上記出力部３００は、上記動作状態測定部１００で測定された動作状態を表示するための表示部３１０と、上記動作状態評価部２００において異常と判定されたことを通報するための通報部３２０とを備えて構成される。

【００４９】上記通報部３２０は、上記判定部２３０で動作状態が異常と判定されたとき少なくともその旨を報知する。好ましくは、異常と判定された項目、動作状態の値、設定されたしきい値を超えた程度などを通報する。

【００５０】上記表示部３１０は、例えば、上記判定部２３０で異常と判定されたとき、当該時点における動作状態を表示する。この表示は、外部から指示を受け付けるまで保持することができる。好ましくは、当該異常発生時点を含む動作状態の履歴を表示する。

【００５１】なお、動作状態を常時表示してもよいことは勿論である。

【００５２】次に、図２を参照して、パケットヘッダ識別・解析部１４０における処理の詳細について説明する。

【００５３】ここでは、端末アドレス、プロトコル、通信リンクおよび再送の有無の識別を例にとって、識別する情報と、データ部の判定位置との関係を中心に説明する。

【００５４】上記端末アドレスは、データ先頭から１２バイト目までのデータで識別する。

【００５５】上記プロトコルは、データの２３バイト目から始まるＩＰヘッダによって識別する。具体的には、ＩＰヘッダの１０バイト目のデータで識別する。例えば、上記１０バイト目のデータの値が、”１”の場合はＩＣＭＰ（Internet Control Message Protocol）であり、”６”の場合はＴＣＰ（Transmission Control Protocol）であり、”１７”の場合はＵＤＰ（User Datagram Protocol）であると識別することができる。

【００５６】上記通信リンクは、通常２０バイト長のＩＰヘッダの直後にあるＴＣＰヘッダを見ることにより識別する。例えば、ＴＣＰヘッダの１～４バイト目の２バイトのポート番号によって識別する。より具体的には、ポート番号が”２１”の場合は、ＦＴＰ（File Transfer Protocol）であり、”２３”の場合は、Ｔｅｌｎｅｔであると識別することができる。

【００５７】上記再送の有無は、ＴＣＰヘッダの５～１２バイト目のシーケンス番号と、アック（ＡＣＫ；acknowledge）番号とによる判断することができる。

【００５８】次に、上記しきい値設定部における処理の詳細について説明する。

【００５９】動作状態測定部で測定された値のうち、性能に関するデータから、同じパターンを繰り返す周期を算出する。この周期は、例えば、対象とするデータの時系列における自己相関を用いて算出することができる。

【００６０】また、過去のある時点t_0までに測定された期間Ｎの時系列データ｛ｆ（ｔ）｜（$t_0-N \leq t \leq t_0$）｝と、これに対して時間差Ｋ（Ｋ＞０）を与えた時系列データ｛ｆ（ｔ）　（$t_0-N-K \leq t \leq t_0-K$）｝との距離を最小とする期間Ｎから、繰り返しの周期を求めてもよい。なお、t_0として、最新のデータが測定された時点（現時点）を選んでもよいことは勿論である。

【００６１】より具体的には、まず、監視装置が稼働してから１日分の時系列データについて、その１日における繰り返し度を求める。繰り返し度は、次式によって定義される。

【００６２】繰り返し度＝Ｍｉｎ［Σ_n｛ｆ（ｔ＋ｎ）－ｆ（ｔ＋ｎ＋Ｋ）｝^{2}］／ｎ

ここで、ｎは、時系列データに含まれる測定ポイント数

であり、Kは、1，2，…，nである。

【0063】さらに、この繰り返し度を稼働してからの期間を変えそれぞれ求め、繰り返し度が最小となる期間を周期と見なす。例えば、稼働してから1日分の時系列データ、1週間分の時系列データ、1ヶ月分の時系列データと期間を変えて、それぞれの期間について繰り返し度を求めて、繰り返し度が最小となる期間を周期とする。

【0064】そして、算出した周期で、性能、応答時間、再送回数、および、エラー発生率の変化を時系列に測定する。この測定した時系列データと、通常動作時の時系列データとの間の距離を求める。時系列データ相互の距離は、例えば、各位相の値を時系列データ相互に比較し、これらの差の二乗の周期における総和として定義する。この定義では、同一時系列データ間の距離は0となる。

【0065】上記の距離から、ネットワークの動作状態の正常／異常の判定基準となるしきい値を、分布関数の異常値と認められる範囲の値と判断する。例えば、標準偏差σの2倍以上を異常範囲とする。これは、正規分布の場合には、全体の事象のうちの約5％の事象を異常とみなすことに相当する。

【0066】次に、図3を参照して、処理フローについて説明する。

【0067】採取したパケットデータをバッファメモリに格納する共に、エラー検出を行う。

【0068】エラー検出では、コリジョン検出、ショート、ロング、アライメント、CRCチェックなどを行う。

【0069】上記コリジョン検出では、多重コリジョン（2重以上）、JAM信号検出、レイトコリジョンを検出する。

【0070】一方、バッファメモリに格納されたパケットデータから、パケットヘッダの識別・解析を行う。

【0071】そして、解析されたパケットヘッダから、性能を測定し、プロトコルを認識し、通信ペアを識別する。

【0072】上記認識したプロトコルに基づいて、プロトコル、パケットデータサイズ、パケットデータ数を求める。

【0073】上記識別した通信ペアに基づいて、状態遷移フロー追跡、応答時間測定、再送回数計測を行う。

【0074】そして、上記計測されたそれぞれのデータを統計処理して、動作状態を定量化する。定量化した動作状態をしきい値設定する。

【0075】また、パケットヘッダの解析から、しきい値と比較し、また解析結果そのものを、動作状態として表示する。

【0076】上記リアルタイムでの応答時間の監視は、次の手順に従って行う。

【0077】IPヘッダおよびTCPヘッダをチェックすることにより、FTP、HTTPなどのようにプロトコルが決められている通信（ヘッダのポート番号から識別することができる）の場合、決められたプロトコルに従って通信が実施されているか否かを、実際の通信の情報をもとに、内蔵しておいた当該プロトコル手順のステータスフロー上をたどることによってチェックする。応答時間の監視は、このレベルにおいて実施する必要がある。これは、通信ペアすべてについて、または、指定されたペアについて、リアルタイムに実施する必要がある。また、監視対象をユーザプログラムの手順とし、ユーザプログラムの通信状態をチェックすることもできる。また、ステータスフローに、新たなエラーについてのステータスフローを追加することによって、検出可能なエラー項目を追加することができる。

【0078】ここで、1パケットのデータ処理に許される時間は、伝送速度が100Mbpsで、64オクテットのフレーム（パケットデータ）が9．6μs間隔で伝送されているとき、

9．6μs－64・8・10ns＝14．7μs

となる。これは、200MHzで動作するインテル社のPentiumプロセッサを用いて、凡そ700ステップのアセンブラプログラムを実行させることができる時間に相当する。

【0079】上述の説明では、ネットワークの異常を検知し、それを報知することを中心に説明した。ここでは、図4を参照して、検知された異常に関連する情報を提供して、ネットワーク障害を回復させる情報を提供することについて説明する。これは、図1における通報部320において実行される。

【0080】まず、図4を参照して、ネットワークに発生する典型的な障害と、応答時間または再送回数に及ぼす影響との関連性について説明する。

【0081】図4において、ネットワークの5つの階層、すなわち、物理層、データリンク層、ネットワーク層、トランスポート層、および、アプリケーション層のそれぞれに典型的に発生する障害と、その障害が発生した際に予想される、応答時間または再送への影響との関連が示されている。

【0082】従って、このような異常が発生した際に、関連する障害の内容を併せて報知することにより障害の回復を支援することができる。

【0083】

【発明の効果】本発明によれば、既に測定されたネットワークの動作状態からネットワークが異常か否かを判定するための基準を設定することができる。

【0084】このため、ネットワークに関する知識や、ネットワーク管理の経験などに依存せずに、対象とするネットワークに応じた基準で異常を検出することが可能となる。

【図面の簡単な説明】

【図１】　ネットワーク監視装置を示すブロック図である。

【図２】　ＩＥＥＥ８０２．３のパケットのデータ構造を示す説明図である。

【図３】　処理を示すフロー図である。

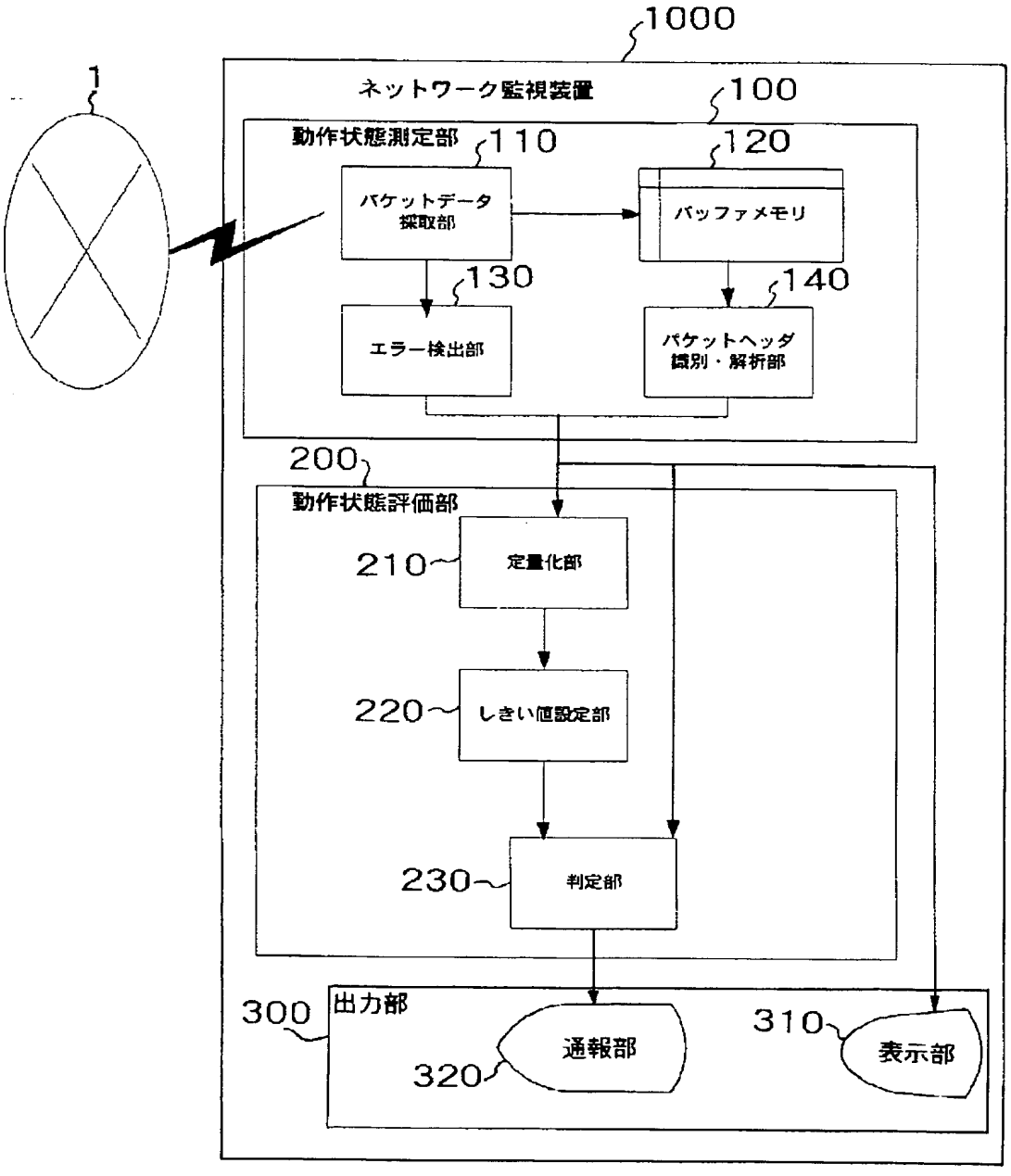
【図４】　障害と、応答時間および再送との関連を示す説明図である。

【符号の説明】

１…対象となるネットワーク、１００…動作状態測定部、１１０…パケットデータ採取部、１２０…バッファメモリ、１３０…エラー検出部、１４０…パケットヘッダ識別・解析部、２００…動作状態評価部、２１０…定量化部、２２０…しきい値設定部、２３０…判定部、３００…出力部、３１０…表示部、３２０…通報部。

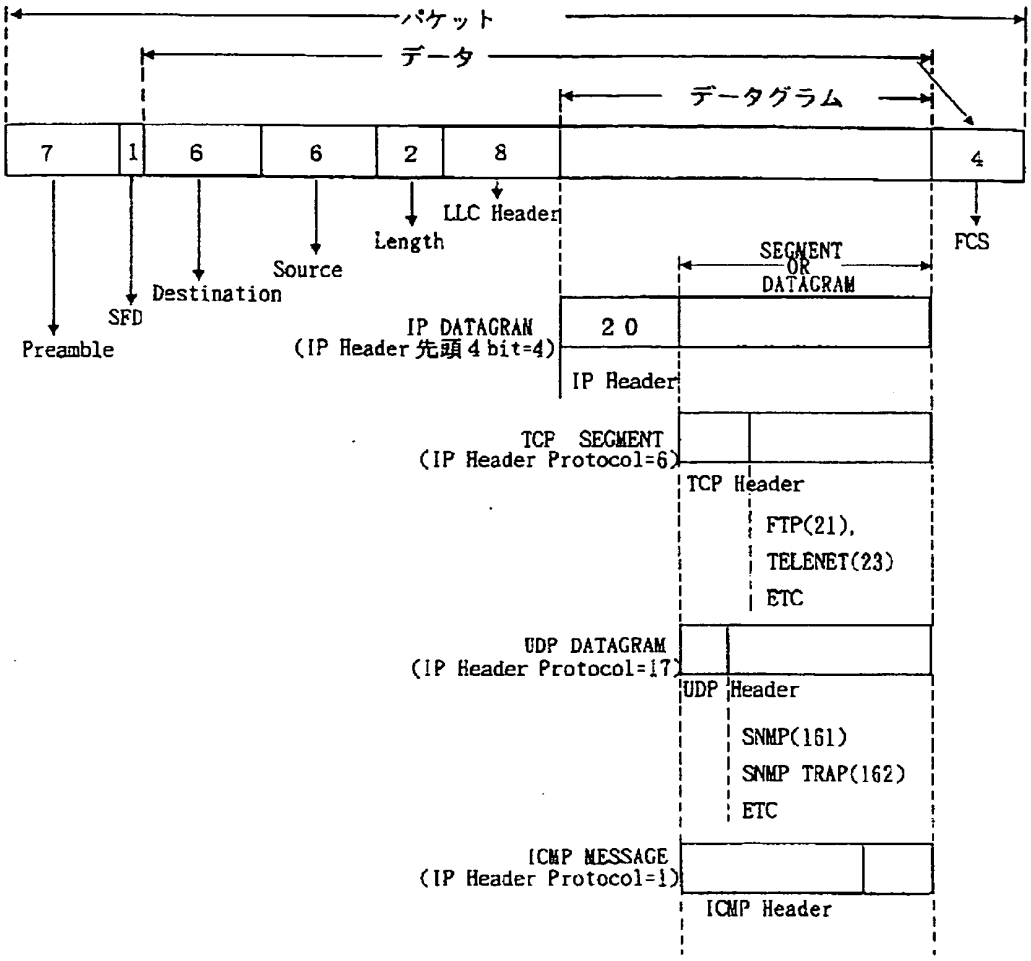
【図１】

図1



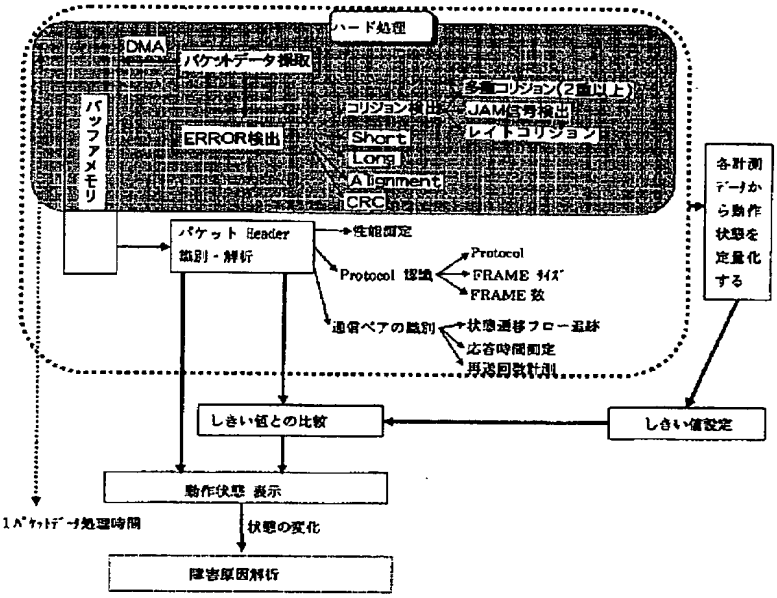
【図2】

図2


パケット
データ
データグラム
7
1
6
6
2
8
4
Preamble
SFD
Destination
Source
Length
LLC Header
FCS
SEGMENT OR DATAGRAM
IP DATAGRAM
(IP Header 先頭4 bit=4)
2 0
IP Header
TCP SEGMENT
(IP Header Protocol=6)
TCP Header
FTP(21),
TELENET(23)
ETC
UDP DATAGRAM
(IP Header Protocol=17)
UDP Header
SNMP(161)
SNMP TRAP(162)
ETC
ICMP MESSAGE
(IP Header Protocol=1)
ICMP Header

【図３】

図3



【図４】

図4

障害と、応答時間および再送との関係

レイヤ	障害内容		応答時間への影響	再送への影響
物理層（レイヤ１）	ケーブル不良	オープン	応答タイムアウト（通信不可）	−
		ショート	応答タイムアウト（通信不可）	−
		終端不良	応答タイムアウト（通信不可）	−
		ノイズ	応答タイム ばらつき大	−
	トランシーバ不良	内部ハードウエア不良	応答タイムアウト（通信不可）	−
		トランシーバ接触不良	応答タイムアウト（通信不可）	
	ＮＩＣ不良		応答タイムアウト（通信不可）	−
	物理規格違反		応答タイムアウト（通信不可）	再送回数増加
	コリジョン多発		応答タイム ばらつき大	−
データリンク層（レイヤ２）	ＭＡＣアドレス重複		−	アプリケーション層での再送回数増加
	Ether タイプ不一致		応答タイムアウト（通信不可）	−
	ブリッジ機能障害／設定ミス		応答タイムアウト（通信不可） 応答タイム ばらつき大	−
ネットワーク層（レイヤ３）	ＩＰアドレス重複		応答タイムアウト（通信不可）	−
	ルーティングエラー		応答タイムアウト（通信不可） 応答タイム ばらつき大	−
	プロトコルタイプ不一致		応答タイムアウト（通信不可）	−
	ルータ機能障害／設定ミス		応答タイムアウト（通信不可） 応答タイム ばらつき大	−
トランスポート層（レイヤ４）	ＴＣＰ機能障害	ウインドウズシンドローム	−	再送回数増加
		ディレイデュプリケート	−	再送回数増加
		再送が多い	−	再送回数増加
	トランスポート実装仕様の相違		応答タイムアウト（通信不可）	−
アプリケーション層（レイヤ５）	再送データの重複／欠落		−	再送回数増加
	データ障害		−	再送回数増加
	ファイル参照不能		応答タイムアウト（通信不可）	−
	ファイル重複		応答タイムアウト（通信不可）	−
	処理速度が遅い		応答タイム ばらつき大	再送回数増加
	ソフトインストールによる通信不良		応答タイムアウト（通信不可）	−

フロントページの続き

(72)発明者　山岸　令和
神奈川県横浜市戸塚区品濃町504番地２
日立電子サービス株式会社内

(72)発明者　武貞　睦治
神奈川県横浜市戸塚区品濃町504番地２
日立電子サービス株式会社内

Fターム(参考) 5K030 GA11 GA16 HA08 HB06 HB28
JA10 MA01 MB01 MC07 MC08
MC09

THIS PAGE BLANK (USPTO)